RECEIVED
CENTRAL FAX CENTER
DEC 12 2005

ZILKA·KOTAB
PC
ZILKA, KOTAB & FEECE™

95 SOUTH MARKET ST., SUITE 420
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	December 12, 2005	**Phone Number**	**Fax Number**
To:	Board of Patent Appeals		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAI1P458/00.164.01 **App. No: 09/809, 073**

Total Number of Pages Being Transmitted, Including Cover Sheet: 41

Message:

Please deliver to the Board of Patent Appeals.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

December 12, 2005

RECEIVED
CENTRAL FAX CENTER

DEC 12 2005

Practitioner's Docket No. NAI1P458/00.164.01 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Tarbotton et al.

Application No.: 09/809,073 Group No.: 2134
Filed: 03/16/2001 Examiner: Simitoski, M.
For: MECHANISMS FOR BANNING COMPUTER PROGRAMS FROM USE

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION–37 C.F.R. § 41.37)

1. Transmitted herewith, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on September 21, 2005.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

12/13/2005 TL0111 00000079 501351 09809073
02 FC:1251 120.00 DA

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*

*(When using Express Mail, the Express Mail label number is **mandatory**; Express Mail certification is optional.)*

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)

_ with sufficient postage as first class mail.

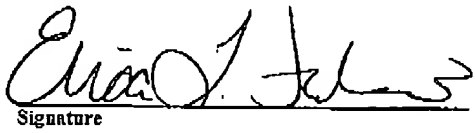
37 C.F.R. § 1.10*

_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ **(mandatory)**

TRANSMISSION

✓ facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.

Date: 12/12/05



Signature

Erica L. Farlow

(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

RECEIVED
CENTRAL FAX CENTER

DEC 12 2005

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant petitions for an extension of time under 37 C.F.R. 1.136 (fees: 37 C.F.R. 1.17(a)(1)-(4)) for one month:

Fee	$120.00

If an additional extension of time is required, please consider this a petition therefor.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$120.00
TOTAL FEE DUE	**$620.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $620.00 to Deposit Account No. 50-1351 (Order No. NAI1P458).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P458).

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172
USA

RECEIVED
CENTRAL FAX CENTER

DEC 12 2005

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of	)
	)
Tarbotton et al.	) Group Art Unit: 2134
	)
Application No. 09/809,073	) Ex: Simitoski, Michael J.
	)
Filed: March 16, 2001	) Date: December 12, 2005
	)
For: MECHANISMS FOR BANNING COMPUTER PROGRAMS FROM USE	)
	)
	)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on September 21, 2005.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS

12/13/2005 TL0111 00000079 501351 09809073
01 FC:1402 500.00 DA

V SUMMARY OF CLAIMED SUBJECT MATTER

VI GROUNDS OF REJECTION PRESENTED FOR REVIEW

VII ARGUMENTS

VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

Since no such proceedings exist, no Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1, 2, 4-8, 10-16, 18-22, 24-30, 32-36, and 38-42

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1, 2, 4-8, 10-16, 18-22, 24-30, 32-36, and 38-42
3. Claims allowed: None
4. Claims rejected: 1, 2, 4-8, 10-16, 18-22, 24-30, 32-36, and 38-42

C. CLAIMS ON APPEAL

The claims on appeal are: 1, 2, 4-8, 10-16, 18-22, 24-30, 32-36, and 38-42

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claims 1, 15 and 29, as shown in Figures 2 and 3, a technique is provided for generating banned program identifying data indicative of at least one computer program to be banned from use. In use, user controlled program specifying logic specifies a computer program to be banned from use, where such computer program comprises an undesired, non-virus computer program (e.g. item 14 of Figure 3). In response to the user controlled program specifying logic, banned program identifying data is generated for the computer program to be banned from use, where the banned program identifying data is operable to control anti computer virus logic to identify computer programs banned from use (e.g. item 44 of Figure 3). Note page 6, lines 19-21 and page 8, lines 12-15, for example.

With respect to a summary of Claims 7, 21 and 35, the above summary is incorporated in part. Note page 6, lines 19-21 and page 8, lines 12-15, for example.

VI GROUNDS OF REJECTION PRESENTED FOR REVIEW (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue #1: The Examiner has rejected Claims 1-2, 4-8, 10-16, 18-22, 24-30, 32-36 and 38-42 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

Issue #2: The Examiner has rejected Claims 21-22 and 24-28 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement.

Issue #3: The Examiner has rejected Claims 1-2, 4-6 and 21 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which appellant regards as the invention.

Issue #4: The Examiner has rejected Claims 1, 4, 6-7, 11-14, 29, 32 and 34 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg.

Issue #5: The Examiner has rejected Claims 2, 8 and 30 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further view of "Bad IDEA", by Peter Szor, in further view of "Cryptography in Everyday Life", by Sarah Simpson.

Issue #6: The Examiner has rejected Claims 5 and 33 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of

"Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further view of "Heuristic Anti-Virus Technology", by Veldman.

Issue #7: The Examiner has rejected Claims 10 and 38 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further view of "Bad IDEA", by Peter Szor, in further view of "Cryptography in Everyday Life", by Sarah Simpson, in further view of Davis, U.S. Patent No. 5,844,986.

Issue #8: The Examiner has rejected Claims 1, 4, 6-7, 11-15, 18, 20-21, 25-29, 32, 34-35 and 39-42 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further view of "Ad-aware", by Lavasoft.

Issue #9: The Examiner has rejected Claims 2, 8, 16, 22, 30 and 36 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further view of "Ad-aware", by Lavasoft, in further view of "Cryptography in Everyday Life", by Sarah Simpson.

Issue #10: The Examiner has rejected Claims 5, 19 and 33 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further view of "Ad-aware", by Lavasoft, in further view of "Heuristic Anti-Virus Technology", by Veldman.

Issue #11: The Examiner has rejected Claims 10, 24 and 38 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further view of "Ad-aware", by Lavasoft, in further view of "Bad IDEA", by Peter Szor, in further view of "Cryptography in Everyday Life", by Sarah Simpson, in further view of Davis, U.S. Patent

No. 5,844,986.

VII ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

Issue #1:

The Examiner has rejected Claims 1-2, 4-8, 10-16, 18-22, 24-30, 32-36 and 38-42 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

The Examiner has stated that the claims contain subject matter which was not described in the specification. Specifically, the Examiner has argued that the banning of an "undesired, non-virus computer program" is not described in the specification.

Appellant respectfully points out the following excerpts from appellant's specification:

Pg. 3, line 29 "banning of undesired computer programs"
Pg. 6, lines 13-14 "...a user specifies the computer programs they wish to ban..."
Pg. 8, line 28 "Figure 3 shows the anti-virus scan taking place before the banned scan..."

Clearly, appellant describes banning undesired programs which may be specified by a user. Thus, as described, any type of program may be banned, including a non-virus computer program. Further, note that examples of non-virus programs are provided on page 1, lines 14-15.

Issue #2:

The Examiner has rejected Claims 21-22 and 24-28 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement.

The Examiner has stated that the claims contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to make and/or use the invention. The Examiner has specifically argued that Claim 21 presents a single method step, which fails to comply with the enablement requirement under MPEP 2164.08(a).

Appellant respectfully asserts that Claim 21 is not to be interpreted under 35 U.S.C. 112, paragraph 6. Specifically, MPEP 2164.08(a) relates to a single means claim "where a means recitation does not appear in combination with another recited element of means." Appellant's Claim 21 does not include a means recitation, but instead claims a method including the following act: "in response to user generated banned program identifying data for said at least one computer program to be banned from use, operating anti computer virus logic to identify computer programs banned from use."

Issue #3:

The Examiner has rejected Claims 1-2, 4-6 and 21 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which appellant regards as the invention.

First, with respect to Claim 1, the Examiner has stated that appellant's claimed "said computer controlling program comprising" is unclear. Appellant respectfully emphasizes the following language from Claim 1, which renders such language clear:

"A computer program product comprising a computer program operable to control a computer to generate banned program identifying data indicative of at least one computer program to be banned from use, said computer controlling program comprising:" (emphasis added).

Second, with respect to Claims 1, 7, 15, 21, 29 and 35, the Examiner has stated that the limitation "undesired" is indefinite because what is undesired to one person is not necessarily undesired to another. Appellant respectfully disagrees that such limitation is indefinite. As claimed, any undesired, non-virus computer program may be banned from use. Appellant respectfully asserts that including a limitation as to the type of undesired program would unduly limit such claim.

Third, with respect to Claims 1, 7, 15, 21, 29 and 35, the Examiner has stated that the limitation "non-virus" program is indefinite because there is no concrete difference between a virus program and a non-virus program. The Examiner has further stated that many non-virus

programs perform unwanted actions on a computer. Appellant respectfully asserts that there is a difference between a virus program and a non-virus program since, for example, a virus program may cause damage by way of the virus whereas a non-virus program may simply be unwanted. Thus, appellant claims banning a non-virus program that is unwanted.

Fourth, with respect to Claim 21, the Examiner has stated that it is unclear if the "user generated program identifying data" is a method operation. Appellant respectfully asserts that Claim 21 is a method claim, and therefore the act is "operating anti computer virus logic" where such step is "in response to user generated banned program," as claimed.

Fifth, with respect to Claim 22, the Examiner has stated that the step of "operating...to identify" has no tangible output. Appellant assumes the Examiner means to refer to Claim 21 since Claim 22 does not recite any sort of "operating." Appellant respectfully asserts that the method of Claim 21 is for "banning from use at least one computer program" and is not for outputting.

Issue #4:

The Examiner has rejected Claims 1, 4, 6-7, 11-14, 29, 32 and 34 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg.

Group #1: Claims 1 and 29

First, appellant notes that the Examiner has failed to even address appellant's claimed "user controlled program specifying logic operable to specify said at least one computer program to be banned from use, said at least one computer program comprising an undesired, non-virus computer program" (see the same or similar, but not identical language in each of the independent claims).

Second, the Examiner has relied on page 31, paragraph 1, page 45 §Submitting files to SARC and page 46 in Symantec to make a prior art showing of appellant's claimed "banned program

identifying data generating logic responsive to said user controlled program specifying logic to generate banned program identifying data for said at least one computer program to be banned from use" (see the same or similar, but not identical language in each of the independent claims).

Specifically, the Examiner has stated that "Symantec discloses a user controlled program identifying data generating logic/Norton AntiVirus to generate banned program identifying data/encrypted suspected virus for said one or more computer programs/suspected viruses to be banned from use/quarantined."

Appellant respectfully asserts that such excerpts only generally define viruses as well as discuss quarantining a file suspected to have a virus. Appellant, on the other hand, specifically claims "generating...banned program identifying data for said at least one computer program to be banned from use." Clearly, quarantining a file suspected to have a virus does not meet any sort of banned program identifying data which identifies a computer program to be banned from use, and especially not where such identifying data is in response to "said user controlled program specifying logic," as claimed by appellant.

Third, the Examiner has relied on pages 10-11 and Figure 1 in Hedberg to make a prior art showing of appellant's claimed "banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use." Specifically, the Examiner has stated that Hedberg teaches "that anti-virus software can be made to detect variations of known viruses and extract identification signatures from them (pages 10-11 & Figure 1) to eliminate the need for the slower traditional approach (page 10, §A neural network virus classifier)."

Appellant respectfully asserts that simply extracting identification signatures of viruses does not meet appellant's claimed "banned program identifying data," which is further emphasized by appellant's remaining claim language to include an "undesired, non-virus computer program" (emphasis added). In addition, anti-virus software that can be made to simply detect variations of known viruses does not meet any sort of "identify[ing] computer programs banned from use" (emphasis added), as specifically claimed.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claims 4 and 32

Appellant notes that the Examiner has failed to make a specific prior art showing of appellant's claimed technique "wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were a computer virus," but instead has merely grouped such claim language under the rejection of the associated independent claims. Appellant respectfully asserts that since none of the references relied on by the Examiner teach "anti computer virus logic [utilized] to identify said computer programs banned from use" (see arguments with respect to Issue #1, Group #1), such references cannot further teach that such identification is done "in a manner substantially the same as if they were a computer virus."

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claims 6, 14 and 34

Appellant notes that the Examiner has failed to make a specific prior art showing of appellant's claimed technique "wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use," but instead has merely grouped such claim language under the rejection of the associated independent claims. Appellant respectfully asserts that none of the references relied on by the Examiner teach any sort of "identifying permitted computer programs," let alone in the specific context claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #4: Claims 7 and 12

The Examiner has relied on pages 10-11 and Figure 1 in Hedberg to make a prior art showing of appellant's claimed "anti computer virus logic responsive to user generated banned program identifying data for said at least one computer program to be banned from use to identify computer programs banned from use." Specifically, the Examiner has stated that Hedberg teaches "that anti-virus software can be made to detect variations of known viruses and extract identification signatures from them (pages 10-11 & Figure 1) to eliminate the need for the slower traditional approach (page 10, §A neural network virus classifier)."

Appellant respectfully asserts that simply extracting identification signatures of viruses does not meet appellant's claimed "banned program identifying data," which is further emphasized by appellant's remaining claim language that such banned program is an "undesired, non-virus computer program" (emphasis added). In addition, anti-virus software that can be made to simply detect variations of known viruses does not meet any sort of "identify[ing] computer programs banned from use" (emphasis added), as claimed.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #5: Claim 11

The Examiner has relied on pages 39-40 in Symantec to make a prior art showing of appellant's claimed technique "wherein when a banned computer program is identified, at least one banned program action is triggered, said banned program action comprising at least one of: (i) issuing an alert message indicating identification of a banned computer program; (ii) denying access to said banned computer program; (iii) encrypting said banned computer program; and (iv) deleting said banned computer program." Appellant respectfully asserts that Symantec only relates to virus alerts, which *teaches away* from appellant's specific claim language, namely "banned program action" (emphasis added), especially when read in view of the fact that appellant's banned program is an "undesired, non-virus computer program" (see Claim 7 from which Claim 11 depends-emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #6: Claim 13

The Examiner has taken official notice to meet appellant's claimed technique "wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use." Specifically, the Examiner has stated that running separate processes on a computer is old and well established in the art of computer application processing, and that thus it would have been obvious to execute the anti computer virus logic as a separate instance. In making such an assertion, it appears that the Examiner has failed to consider the full weight of appellant's claim language. Specifically, appellant claims "anti computer virus logic [that] is executable as a separate instance solely to identify computer programs banned from use"

(emphasis added), such that utilizing anti computer virus logic to identify computer programs banned from use may be executed separate from any other execution done by the anti computer virus logic, such as for example, running a virus scan.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue #5:

The Examiner has rejected Claims 2, 8 and 30 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further view of "Bad IDEA", by Peter Szor, in further view of "Cryptography in Everyday Life", by Sarah Simpson.

Group #1: Claims 2, 8 and 30

Appellant respectfully asserts that Claims 2, 8 and 30 are not met by the references relied on by the Examiner by virtue of the arguments made above with respect to Issue #1, Group #1 and #4.

Issue #6:

The Examiner has rejected Claims 5 and 33 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further view of "Heuristic Anti-Virus Technology", by Veldman.

Group #1: Claims 5 and 33

The Examiner has relied on §1 and §2.1 in Veldman to make a prior art showing of appellant's claimed technique "wherein said banned program identifying data includes heuristic data

identifying at least one behavioral characteristic of at least one computer program banned from use such that variants of said at least one computer program banned from use that share said behavioral characteristics may also be identified." Appellant respectfully asserts that describing a generic detection method for identifying viruses does not meet appellant's specific claim language, namely "identifying at least one behavioral characteristic of at least one computer program banned from use" (emphasis added), and especially not when read in view of the fact that appellant's computer program banned from use is an "undesired, non-virus computer program" (see independent claims from which such claim language depends).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue #7:

The Examiner has rejected Claims 10 and 38 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further view of "Bad IDEA", by Peter Szor, in further view of "Cryptography in Everyday Life", by Sarah Simpson, in further view of Davis, U.S. Patent No. 5,844,986.

Group #1: Claims 10 and 38

The Examiner has relied on Col. 1, lines 32-45 and 63-67 in Davis to make a prior art showing of appellant's claimed technique "wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted." Appellant notes however that such excerpts disclose "imposing an authentication and validation process before the contents of the BIOS flash memory are modified" in order to prevent viruses from corrupting the BIOS. Clearly, such teaching does not even suggest "decrypted banned program identifying data," let alone where such data is "stored within a secured memory region once decrypted," as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue #8:

The Examiner has rejected Claims 1, 4, 6-7, 11-15, 18, 20-21, 25-29, 32, 34-35 and 39-42 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further view of "Ad-aware", by Lavasoft.

Group #1: Claims 1, 15 and 29

First, the Examiner has relied on page 31, paragraph 1, page 45 §Submitting files to SARC and page 46 in Symantec to make a prior art showing of appellant's claimed "banned program identifying data generating logic responsive to said user controlled program specifying logic to generate banned program identifying data for said at least one computer program to be banned from use" (see the same or similar, but not identical language in each of the independent claims).

Specifically, the Examiner has stated that "Symantec discloses a user controlled program identifying data generating logic/Norton AntiVirus to generate banned program identifying data/encrypted suspected virus for said one or more computer programs/suspected viruses to be banned from use/quarantined."

Appellant respectfully asserts that such excerpts only generally define viruses as well as discuss quarantining a file suspected to have a virus. Appellant, on the other hand, specifically claims "generating...banned program identifying data for said at least one computer program to be banned from use." Clearly quarantining a file suspected to have a virus does not meet any sort of banned program identifying data which identifies a computer program to be banned from use, and especially not where such identifying data is in response to "said user controlled program specifying logic," as claimed by appellant.

Second, the Examiner has relied on pages 10-11 and Figure 1 in Hedberg to make a prior art showing of appellant's claimed "banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use." Specifically, the Examiner has stated that Hedberg teaches "that anti-virus software can be made to detect variations of known viruses and extract identification signatures from them (pages 10-11 & Figure 1) to eliminate the need for the slower traditional approach (page 10, §A neural network virus classifier)."

Appellant respectfully asserts that simply extracting identification signatures of viruses does not meet appellant's claimed "banned program identifying data," which is further emphasized by appellant's remaining claim language to include an "undesired, non-virus computer program" (emphasis added). In addition, anti-virus software that can be made to simply detect variations of known viruses does not meet any sort of "identify[ing] computer programs banned from use" (emphasis added), as specifically claimed.

Third, the Examiner has relied on pg. 1 in Lavasoft to make a prior art showing of appellant's claimed "user controlled program specifying logic operable to specify said at least one computer program to be banned from use, said at least one computer program comprising an undesired, non-virus computer program." Specifically, the Examiner has argued that Lavasofts teaching of scanning for spyware to remove it and monitoring memory and registries for spyware that attempts to install or change a computer system meets appellant's specific claim language.

Appellant respectfully asserts that scanning for spyware to remove it and monitoring spyware that changes a computer system does meet appellant's specific claim language. Simply nowhere in Lavasoft is there any teaching of "specify[ing] ... at least one computer program to be banned from use," as claimed by appellant (emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claims 4, 18 and 32

Appellant notes that the Examiner has failed to make a specific prior art showing of appellant's claimed technique "wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were a computer virus," but instead has merely grouped such claim language under the rejection of the associated independent claims. Appellant respectfully asserts that since none of the references relied on by the Examiner teach "anti computer virus logic [utilized] to identify said computer programs banned from use" (see arguments with respect to Issue #8, Group #1), such references cannot further teach that such identification is done "in a manner substantially the same as if they were a computer virus."

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claims 6, 14, 20, 28, 34 and 42

Appellant notes that the Examiner has failed to make a specific prior art showing of appellant's claimed technique "wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use," but instead has merely grouped such claim language under the rejection of the associated independent claims. Appellant respectfully asserts that none of the references relied on by the Examiner teach any sort of "identifying permitted computer programs," let alone in the specific context claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #4: Claims 7, 12, 21, 26, 35, and 40

The Examiner has relied on pages 10-11 and Figure 1 in Hedberg to make a prior art showing of appellant's claimed "anti computer virus logic responsive to user generated banned program identifying data for said at least one computer program to be banned from use to identify computer programs banned from use." Specifically, the Examiner has stated that Hedberg teaches "that anti-virus software can be made to detect variations of known viruses and extract identification signatures from them (pages 10-11 & Figure 1) to eliminate the need for the slower traditional approach (page 10, §A neural network virus classifier)."

Appellant respectfully asserts that simply extracting identification signatures of viruses does not meet appellant's claimed "banned program identifying data," which is further emphasized by appellant's remaining claim language that such banned program is an "undesired, non-virus computer program" (emphasis added). In addition, anti-virus software that can be made to simply detect variations of known viruses does not meet any sort of "identify[ing] computer programs banned from use" (emphasis added), as claimed.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #5: Claims 11, 25 and 39

The Examiner has relied on pages 39-40 in Symantec to make a prior art showing of appellant's claimed technique "wherein when a banned computer program is identified, at least one banned program action is triggered, said banned program action comprising at least one of: (i) issuing an alert message indicating identification of a banned computer program; (ii) denying access to said banned computer program; (iii) encrypting said banned computer program; and (iv) deleting said banned computer program." Appellant respectfully asserts that Symantec only relates to virus alerts, which *teaches away* from appellant's specific claim language, namely "banned program

action" (emphasis added), especially when read in view of the fact that appellant's banned program is an "undesired, non-virus computer program" (see Claim 7 from which Claim 11 depends-emphasis added).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #6: Claims 13, 27 and 41

The Examiner has taken official notice to meet appellant's claimed technique "wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use." Specifically, the Examiner has stated that running separate processes on a computer is old and well established in the art of computer application processing, and that thus it would have been obvious to execute the anti computer virus logic as a separate instance. In making such an assertion, it appears that the Examiner has failed to consider the full weight of appellant's claim language. Specifically, appellant claims "anti computer virus logic [that] is executable as a separate instance solely to identify computer programs banned from use" (emphasis added), such that utilizing anti computer virus logic to identify computer programs banned from use may be executed separate from any other execution done by the anti computer virus logic, such as for example, running a virus scan.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue #9:

The Examiner has rejected Claims 2, 8, 16, 22, 30 and 36 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further

view of "Ad-aware", by Lavasoft, in further view of "Cryptography in Everyday Life", by Sarah Simpson.

Group #1: Claims 2, 8, 16, 22, 30 and 36

Appellant respectfully asserts that Claims 2, 8 and 30 are not met by the references relied on by the Examiner by virtue of the arguments made above with respect to Issue #8, Group #1 and #4.

Issue #10:

The Examiner has rejected Claims 5, 19 and 33 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further view of "Ad-aware", by Lavasoft, in further view of "Heuristic Anti-Virus Technology", by Veldman.

Group #1: Claims 5, 19 and 33

The Examiner has relied on §1 and §2.1 in Veldman to make a prior art showing of appellant's claimed technique "wherein said banned program identifying data includes heuristic data identifying at least one behavioral characteristic of at least one computer program banned from use such that variants of said at least one computer program banned from use that share said behavioral characteristics may also be identified." Appellant respectfully asserts that describing a generic detection method for identifying viruses does not meet appellant's specific claim language, namely "identifying at least one behavioral characteristic of at least one computer program banned from use" (emphasis added), and especially not when read in view of the fact that appellant's computer program banned from use is an "undesired, non-virus computer program" (see independent claims from which such claim language depends).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue #11:

The Examiner has rejected Claims 10, 24 and 38 under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation, in view of "Combating Computer Viruses: IBM's New Computer Immune System", by Hedberg, in further view of "Ad-aware", by Lavasoft, in further view of "Bad IDEA", by Peter Szor, in further view of "Cryptography in Everyday Life", by Sarah Simpson, in further view of Davis, U.S. Patent No. 5,844,986.

Group #1: Claims 10, 24 and 38

The Examiner has relied on Col. 1, lines 32-45 and 63-67 in Davis to make a prior art showing of appellant's claimed technique "wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted." Appellant notes however that such excerpts disclose "imposing an authentication and validation process before the contents of the BIOS flash memory are modified" in order to prevent viruses from corrupting the BIOS. Clearly such teaching does not even suggest "decrypted banned program identifying data," let alone where such data is "stored within a secured memory region once decrypted" as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A computer program product comprising a computer program operable to control a computer to generate banned program identifying data indicative of at least one computer program to be banned from use, said computer controlling program comprising:
(i) user controlled program specifying logic operable to specify said at least one computer program to be banned from use, said at least one computer program comprising an undesired, non-virus computer program; and
(ii) banned program identifying data generating logic responsive to said user controlled program specifying logic to generate banned program identifying data for said at least one computer program to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use.

2. (Original) A computer program product as claimed in claim 1, wherein said banned program identifying data is encrypted with a private key.

3. (Cancelled)

4. (Original) A computer program product as claimed in claim 1, wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were a computer virus.

5. (Previously Presented) A computer program product as claimed in claim 4, wherein said banned program identifying data includes heuristic data identifying at least one behavioral characteristic of at least one computer program banned from use such that variants of said at least one computer program banned from use that share said behavioral characteristics may also be identified.

6. (Original) A computer program product as claimed in claim 1, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

7. (Previously Presented) A computer program product comprising a computer program operable to control a computer to ban from use at least one computer program, said at least one computer program comprising an undesired, non-virus computer program, said computer program comprising:

(i) anti computer virus logic responsive to user generated banned program identifying data for said at least one computer program to be banned from use to identify computer programs banned from use.

8. (Original) A computer program product as claimed in claim 7, wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use.

9. (Cancelled)

10. (Original) A computer program product as claimed in claim 8, wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

11. (Previously Presented) A computer program product as claimed in claim 7, wherein when a banned computer program is identified, at least one banned program action is triggered, said banned program action comprising at least one of:

(i) issuing an alert message indicating identification of a banned computer program;

(ii) denying access to said banned computer program;

(iii) encrypting said banned computer program; and

(iv) deleting said banned computer program.

12. (Original) A computer program product as claimed in claim 7, wherein said anti computer virus logic responses to an absence of said user generated banned program identifying data by performing at least one of:

(i) issuing an alert message indicating an absence of said user generated banned program identifying data;

(ii) restoring said user generated banned program identifying data from a remote source;

(iii) disabling a computer upon which said anti computer virus logic is executing.

13. (Original) A computer program product as claimed in claim 7, wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use.

14. (Original) A computer program product as claimed in claim 7, wherein said user generated banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

15. (Previously Presented) A method of generating banned program identifying data indicative of at least one computer program to be banned from use, said method comprising the steps of:

(i) user specifying at least one computer program to be banned from use, said at least one computer program comprising an undesired, non-virus computer program; and

(ii) generating banned program identifying data for said at least one computer program to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use.

16. (Original) A method as claimed in claim 15, wherein said banned program identifying data is encrypted with a private key.

17. (Cancelled)

18. (Original) A method as claimed in claim 15, wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were a computer virus.

19. (Previously Presented) A method as claimed in claim 18, wherein said banned program identifying data includes heuristic data identifying at least one behavioral characteristic of at least one computer program banned from use such that variants of said at least one computer program banned from use that share said behavioral characteristics may also be identified.

20. (Original) A method as claimed in claim 15, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

21. (Previously Presented) A method for banning from use at least one computer program, said at least one computer program comprising an undesired, non-virus computer program, said method comprising the step of:

(i) in response to user generated banned program identifying data for said at least one computer program to be banned from use, operating anti computer virus logic to identify computer programs banned from use.

22. (Original) A method as claimed in claim 21, wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use.

23. (Cancelled)

24. (Original) A method as claimed in claim 22, wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

25. (Previously Presented) A method as claimed in claim 21, wherein when a banned computer program is identified, at least one banned program action is triggered, said banned program action comprising at least one of:

(i) issuing an alert message indicating identification of a banned computer program;

(ii) denying access to said banned computer program;

(iii) encrypting said banned computer program; and

(iv) deleting said banned computer program.

26. (Original) A method as claimed in claim 21, wherein said anti computer virus logic responses to an absence of said user generated banned program identifying data by performing at least one of:

(i) issuing an alert message indicating an absence of said user generated banned program identifying data;

(ii) restoring said user generated banned program identifying data from a remote source;

(iii) disabling a computer upon which said anti computer virus logic is executing.

27. (Original) A method as claimed in claim 21, wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use.

28. (Original) A method as claimed in claim 21, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

29. (Previously Presented) Apparatus for generating banned program identifying data indicative of at least one computer program to be banned from use, said apparatus comprising:

(i) a user controlled program specifier operable to specify at least one computer program to be banned from use, said at least one computer program comprising an undesired, non-virus computer program; and

(ii) banned program identifying data generator responsive to said user controlled program specifier to generate banned program identifying data for said at least one computer program to

be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use.

30. (Original) Apparatus as claimed in claim 29, wherein said banned program identifying data is encrypted with a private key.

31. (Cancelled)

32. (Original) Apparatus as claimed in claim 29, wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were a computer virus.

33. (Previously Presented) Apparatus as claimed in claim 32, wherein said banned program identifying data includes heuristic data identifying at least one behavioral characteristic of at least one computer program banned from use such that variants of said at least one computer program banned from use that share said behavioral characteristics may also be identified.

34. (Original) Apparatus as claimed in claim 29, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

35. (Previously Presented) Apparatus for banning from use at least one computer program, said at least one computer program comprising an undesired, non-virus computer program, said apparatus comprising:

(i) an anti computer virus system responsive to user generated banned program identifying data for said at least one computer program to be banned from use to identify computer programs banned from use.

36. (Original) Apparatus as claimed in claim 35, wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use.

37. (Cancelled)

38. (Original) Apparatus as claimed in claim 36, wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

39. (Previously Presented) Apparatus as claimed in claim 35, wherein when a banned computer program is identified, at least one banned program action is triggered, said banned program action comprising at least one of:

(i) issuing an alert message indicating identification of a banned computer program;

(ii) denying access to said banned computer program;

(iii) encrypting said banned computer program; and

(iv) deleting said banned computer program.

40. (Original) Apparatus as claimed in claim 35, wherein said anti computer virus system responses to an absence of said user generated banned program identifying data by performing at least one of:

(i) issuing an alert message indicating an absence of said user generated banned program identifying data;

(ii) restoring said user generated banned program identifying data from a remote source;

(iii) disabling a computer upon which said anti computer virus logic is executing.

41. (Original) Apparatus as claimed in claim 35, wherein said anti computer virus system is executable as a separate instance solely to identify computer programs banned from use.

42. (Original) Apparatus as claimed in claim 35, wherein said user generated banned program identifying data comprises data identifying permitted computer programs with all computer

programs not matching a permitted computer program being identified as a computer program banned from use.

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P458).

Respectfully submitted,

By: _____ Date: 12/12/05

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660